UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, Inc.
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006

Plaintiff,

v.

NATIONAL SECURITY AGENCY
9800 Savage Road
Fort Meade, M.D. 20755

CENTRAL INTELLIGENCE AGENCY
Washington, D.C. 20505

DEPARTMENT OF DEFENSE
1400 Defense Pentagon
Washington, D.C. 20301-1400

DEPARTMENT OF STATE
2201 C Street NW
Washington, D.C. 20520

Defendants.

COMPLAINT

Plaintiff Freedom Watch, Inc. brings this action against the National Security Agency, the Central Intelligence Agency, the Department of Defense, and the Department of State, to compel compliance with the Freedom of Information Act, 5 U.S.C. § 552 ("FOIA"). As grounds therefor, Plaintiff alleges as follows.

JURISDICTION AND VENUE

1. The Court has jurisdiction over this action pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. §1331. Venue is proper in this district pursuant to 28 U.S.C. §1391(e).

PARTIES

2. Plaintiff Freedom Watch is a non-profit, public interest foundation organized under the laws of the District of Columbia and having its principal place of business at 2020 Pennsylvania Ave., NW Suite 345, Washington, DC, 20006. Plaintiff seeks to promote openness within the federal government and their actions.

3. Defendants are agencies of the United States Government. Defendants have possession, custody, and control of records to which Plaintiff seeks access.

STATEMENT OF FACTS

4. On or about June 1, 2012 Plaintiff sent a FOIA request, via facsimile and the mail, to defendants seeking records about leaked information as set forth below and attached as Exhibit 1. Specifically, Plaintiff sought:

"...all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;

2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger

4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reasons for "leaking" the information;

5) Any and all information that refer or relate to the decision to "leak" the above previously classified information;

6) Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information."

(Exhibit 1)(Given the identical requests sent to all Defendants, only the page of FOIA requests for Defendants CIA, Dept. of Defense, and Dept. of State are included.)

5. Plaintiff requested a fee waiver and expedited processing in accordance with the procedures set forth under the regulations of each agency.

6. The records Plaintiff seeks are of urgent importance and are in the extreme public interest. The American people need to be informed expeditiously through disseminations by Freedom Watch of the requested records, as it affects their immediate well being, economically and otherwise.

7. Between June 11, 2012 and June 12, 2012 Plaintiff received letters through the mail from Defendants acknowledging receipt of Plaintiff's FOIA requests.

8. Pursuant to 5 U.S.C. § 552 (a)(6)(A) Defendant was required and failed to respond timely to Plaintiff's FOIA request.

9. As of the date of this Complaint, Defendants have failed to produce any records responsive to the request or demonstrate that the responsive records are exempt from production. Nor have they indicated whether or when any responsive records will be produced, nor has a fee waiver been granted. In sum, Defendants have failed to respond to the requests in any substantive manner.

10. Because Defendants failed to comply with the time limits set forth in 5 U.S.C. §552(a)(6)(C), Plaintiff is deemed to have exhausted any and all administrative remedies with respect of its FOIA request, pursuant to 5 U.S.C. § 552(a)(6)(C).

COUNT 1

(Violation of FOIA, 5 U.S.C § 552, et. seq.)

11. Plaintiff realleges paragraphs1 through 10 as if fully stated herein.

12. Defendants are unlawfully withholding records requested by Plaintiff pursuant to 5 U.S.C. § 552, et. seq.

13. Plaintiff is being irreparably harmed by reason of Defendants' unlawful withholding of requested records, and Plaintiff will continue to be irreparably harmed unless Defendants are compelled to conform to the requirements of this law.

WHEREFORE, Plaintiff respectfully requests that the Court: (1) Order Defendants to conduct expedited searches for any and all responsive records to Plaintiff's FOIA request and demonstrate that they employed search methods reasonably likely to lead to the discovery of records responsive to Plaintiff's FOIA request; (2) order Defendants to expeditiously produce, by a date certain, any and all records responsive to Plaintiff's FOIA request and a Vaughn index of any responsive records withheld under claim of exemption; (3) enjoin Defendants from continuing to withhold any and all records responsive to Plaintiff's FOIA request; (4) grant Plaintiff an award of attorney's fees and other litigation costs reasonably incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E); and (5) grant Plaintiff any other relief as the Court deems just or proper.

Dated: June 27, 2012

Respectfully Submitted,

Larry Klayman, Esq.
D.C. Bar No. 334581
Chairman & Chief Counsel
Freedom Watch
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

Exhibit 1

FREEDOM WATCH
www.FreedomWatchUSA.org
World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 leklayman@gmail.com

Via Mail and Fax

June 1, 2012

National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the National Security Agency produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;

2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger

4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reasons for "leaking" the information;

5) Any and all information that refer or relate to the decision to "leak" the above previously classified information;

6) Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information.

If any responsive record or portion thereof is claimed to be exempt from production under FOIA, sufficient identifying information (with respect to each allegedly exempt record or portion thereof) must be provided to allow the assessment of the propriety of the claimed exemption. *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), *cert denied*, 415 U.S. 977 (1974). Additionally, pursuant to law, any reasonably segregable portion of a responsive record must be provided after redaction of any allegedly exempt material. 5 U.S.C. §552(b).

I request a waiver of all fees for this request under 5. U.S.C. § 552(a)(4)(A)(iii). Disclosure of the requested information to Freedom Watch is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest. The Islamic Republic of Iran's goal of obtaining nuclear weapons affects the safety of both Israel and the United States, thus putting American citizens at risk. Furthermore, the release of classified information by any particular individual within the executive branch, including the president, further endangers the American people and raises a spectre of corruption within the federal government that must be examined. Freedom Watch is engaged in the active dissemination of public information as is evident by our ongoing public interest legal work and continual fight against corruption within the United States government, and international cases, particularly with regard to Iran. Freedom Watch's website, freedomwatchusa.org serves as the primary means of disseminating that information, and is seen by millions of people annually. In addition, officials of Freedom Watch frequently appear on radio and television to disseminate important information to the public.

Furthermore, on behalf of Freedom Watch I am requesting expedited handling as provided in Department of Defense FOIA Regulation 54000.7-R because there is an urgency to inform the public about an actual or alleged federal government activity. Iran is reportedly on the verge of acquiring nuclear weapons and Israel is reportedly

on the verge of attacking it to prevent their acquisition. The issue of a possible attack on Iran is of importance to the American people because Iran's acquiring of nuclear weapons places the safety of the American people as well as the safety of our allies in jeopardy. This war can break out any time because a strike is needed before Iran can gain the capability to build a bomb. This fact is also evidenced in the article mentioned above. There is an immediate clear and present danger to U.S. citizens, American military personnel.

The above mentioned "leaked" information is no longer in effect classified, if it ever was, as it was disclosed to the public by Mr. Sanger and The New York Times with the aid and complicity of President Obama and his administration. It was disclosed for political purposes to further President Obama's 2012 re-election campaign.

On behalf of Freedom Watch, I look forward to receiving the requested documents and a full fee waiver within ten (10) business days. You may have them delivered to the above address.

Sincerely,

Larry Klayman, Esq.
Chairman and General Counsel
2020 Pennsylvania Ave, N.W., Suite 345
Washington, D.C. 20006
leklayman@gmail.com

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow

their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

"We discussed the irony, more than once," one of his aides said. Another said that the administration was resistant to developing a "grand theory for a weapon whose possibilities they were still discovering." Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America's European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation's nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran's president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran's systems — even

tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America's nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.

The goal was to gain access to the Natanz plant's industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to "phone home" — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low; one participant said the goal was simply to "throw a little sand in the gears" and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence of cyberskills set to work developing the enormously complex computer worm th the attacker from within.

The unusually tight collaboration with Israel was driven by two imperatives. I a part of its military, had technical expertise that rivaled the N.S.A.'s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to

be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called "the bug." But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran's P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed "destructive testing," essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department's national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. After several false starts, it worked. One day, toward the end of Mr. Bush's term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran's underground enrichment plant.

"Previous cyberattacks had effects limited to other computers," Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction," rather than just slow another computer, or hack into it to steal data.

"Somebody crossed the Rubicon," he said.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. "That was our holy grail," one of the architects of the plan said. "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. "The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence," one of the architects of the early attack said.

The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. "This may have been the most brilliant part of the code," one American official said.

Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.

"The intent was that the failures should make them feel they were stupid, which is what happened," the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole "stands" that linked 164 machines, looking for signs of sabotage in all of them. "They overreacted," one official said. "We soon discovered they fired people."

Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results. There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.

But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice.

The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America's defenses and announced it with great fanfare in the East Room.

What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the "horse blanket," a giant foldout schematic diagram of Iran's nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he

would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.

"From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision," a senior administration official said. "And it's safe to say that whatever other activity might have been under way was no exception to that rule."

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

"We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself "in the wild," where computer security experts can dissect it and figure out its purpose.

"I don't think we have enough information," Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran's oil revenues.

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, "has been overwhelmingly on one country." There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. "We've considered a lot more attacks than we have gone ahead with," one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

This article is adapted from "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," to be published by Crown on Tuesday.

FREEDOM WATCH
www.FreedomWatchUSA.org
World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 leklayman@gmail.com

Via Mail and Fax

June 1, 2012

Office of Information Programs and Services
A/GIS/IPS/RL
U. S. Department of State
Washington, D. C. 20522-8100

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Department of State produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;

2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger

FREEDOM WATCH
www.FreedomWatchUSA.org
World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 leklayman@gmail.com

Via Mail and Fax

June 1, 2012

Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Central Intelligence Agency produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;

2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

FREEDOM WATCH
www.FreedomWatchUSA.org
World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 leklayman@gmail.com

Via Mail and Fax

June 1, 2012

OSD/JS FOIA Requester Service Center
Office of Freedom of Information
1155 Defense Pentagon
Washington, DC 20301-1155

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Department of Defense produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;

2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;